SOYEZ RÉEL À PROPOS DE LA RÉSILIENCE IDENTITAIRE: LE NOUVEL IMPÉRATIF POUR LA CYBERDÉFENSE DES ENTREPRISES

La plupart des violations étant liées à des identifiants compromis, les organisations doivent aller au-delà de la prévention pour construire une véritable résilience en matière d'identité.

Les systèmes d'identité comme Microsoft Active Directory (AD), Entra ID et Okta sont des éléments clés de l'informatique d'entreprise : ils authentifient les utilisateurs et contrôlent l'accès aux systèmes critiques. De la connexion aux postes de travail à l'accès physique aux bâtiments, ces systèmes d'identité garantissent le bon fonctionnement des organisations, ce qui en fait une cible de choix pour les cybercriminels.

Mais voici ce que la plupart des organisations ignorent : les approches traditionnelles de protection et de récupération des systèmes d'identité sont fondamentalement inadaptées face aux menaces actuelles. La résilience des identités va bien au-delà de la simple protection des données : elle exige une stratégie globale qui anticipe les attaques sophistiquées et permette un retour rapide à un état fiable, au rythme des activités de l'entreprise.

Lorsque les systèmes d'identité sont indisponibles ou compromis, cela peut perturber gravement les applications et les processus métiers, bloquant l'accès des utilisateurs aux ressources et systèmes vitaux.

C’est là que la résilience des identités devient cruciale. La résilience des identités ne se limite pas à la sauvegarde de votre annuaire ; il s’agit de construire une infrastructure d’identité capable de résister aux attaques sophistiquées, de s’y adapter et de s’en remettre rapidement, tout en assurant la continuité des activités.

IDENTITÉ: LA SURFACE D'ATTAQUE PRINCIPALE

La réalité de la cyberguerre moderne est que l'infrastructure d'identité est devenue le principal champ de bataille. Les attaquants ne s'introduisent plus de force : ils se connectent en utilisant des identifiants compromis pour obtenir un accès légitime. Une fois à l'intérieur, ils peuvent se déplacer discrètement dans l'environnement, accroître les privilèges et saper les mécanismes de récupération avant même que quiconque ne réalise ce qui s'est passé.

Les statistiques dressent un tableau alarmant du paysage actuel des menaces.

88%

des attaques d'applications Web utilisant des identifiants volés.[1]

82%

des organisations ont subi au moins une attaque basée sur l'identité dans les 12 derniers mois.[2]

57%

de cyberattaques ont débuté par une usurpation d'identité.[3]

1 Rapport d'enquête sur les violations de données de 2025,Verizon
2 Rapport sur l'avenir de la sécurité de l'identité 2025, ConductorOne
3 Rapport sur la crise d'identité, Varonis

LES ATTAQUES D'IDENTITÉ SONT DISCRÈTES, ÉVOLUTIVES, ET DIFFICILES À DÉTECTER

Les attaques basées sur l'identité sont particulièrement dangereuses en raison de leur subtilité. En usurpant l'identité d'utilisateurs légitimes, les attaquants peuvent se fondre dans les activités normales et contourner les défenses traditionnelles.

Malgré la diversité des tactiques utilisées, ces attaques partagent un objectif commun : exploiter l'identité pour obtenir un accès autorisé et rester indétectable.

Vol d'identifiants

(hameçonnage, vol de jetons, logiciels malveillants)

Élévation de privilèges par le biais de mauvaises configurations

Abus de permissions excessives

Persistance via la manipulation d'annuaires ou des comptes de porte dérobée

Aujourd'hui, l'automatisation permise par l'IA a accéléré ces attaques, permettant une élévation de privilèges et une propagation latérale plus rapides. Les organisations disposent de moins de temps que jamais pour détecter une compromission, en limiter l'impact et se rétablir.

LA COMPLEXITÉ DE LA PROTECTION DES IDENTITÉS

La prolifération des identités a des répercussions sur la visibilité et le contrôle.

Les informations d'identité sont omniprésentes : systèmes sur site, plateformes cloud, applications SaaS. Cette explosion de données d'identité accroît les lacunes en matière de visibilité et les points d'entrée potentiels pour les attaquants.

Les outils cloisonnés créent des angles morts.

La gestion des risques liés à l'identité s'effectue à travers des outils et des équipes non connectés, ce qui rend plus difficile la priorisation, le repérage précoce des problèmes et plus lent à réagir en cas d'incidents.

La complexité augmente la surface d'attaque.

Les entreprises modernes fonctionnent avec des systèmes d'identité complexes, interconnectés et interdépendants, répartis entre des environnements sur site et dans le cloud, ce qui élargit la surface d'attaque et rend la récupération plus difficile.

Absence de reprise résiliente.

De nombreuses méthodes de récupération sont lentes et complexes, obligeant souvent à s'appuyer sur des sauvegardes compromises ou sur des reconstructions manuelles, ce qui prolonge les temps d'arrêt et augmente les risques.

Ces tendances convergent pour créer une nouvelle réalité opérationnelle :

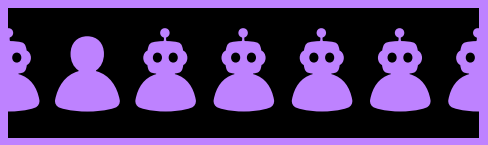
L'identité est la couche la plus ciblée de l'entreprise.

Les environnements de gestion des identités et des accès (IAM) sont plus complexes et interconnectés que jamais.

Les attaques sont plus rapides, plus silencieuses et plus difficiles à détecter.

Une reprise rapide et sans encombre est à la fois plus cruciale et plus difficile qu'auparavant.

144:1



rapport entre les identités non humaines et les identités humaines.[4]

75%

les organisations utilisent plusieurs fournisseurs d'identité pour gérer l'identité d'entreprise.[5]

4 Rapport sur les risques liés aux identités non humaines (NHI) et aux secrets pour le premier semestre 2025, Entro

5 Enquête sur l'état de l'identité multicloud, Strata

L'IMPACT DES ATTAQUES BASÉES SUR L'IDENTITÉ SUR LES ORGANISATIONS

L'importance de la résilience des identités est manifeste lorsqu'on considère son impact en cascade sur les autres charges de travail. Applications, systèmes de fichiers, services de messagerie et bases de données dépendent tous de l'identité pour une authentification et un accès utilisateur corrects.

Lorsque les systèmes d'identité sont indisponibles ou ne sont pas fiables :

Les employés et les clients ne peuvent pas s'authentifier.

Les applications et les services deviennent indisponibles.

Les délais de rétablissement peuvent s'étendre sur plusieurs semaines ou plusieurs mois.

La résilience de l'identité reconnaît cette dépendance fondamentale. Étant donné que presque tout dans les entreprises modernes repose sur l'identité, la mise en place d'une infrastructure d'identité résiliente devient la pierre angulaire de

la résilience organisationnelle. Cela va bien au-delà de la simple restauration des systèmes d'identité après une attaque.

En mettant en place des pratiques de résilience d'identité, les organisations peuvent mieux contrôler leurs réseaux et systèmes même pendant des attaques actives, appliquer des politiques de sécurité et d'accès aux données et fournir une base stable qui favorise la reprise rapide des autres systèmes et services.

LE COÛT DE COMPROMIS D'IDENTITÉ

Pertes financières

Les attaques basées sur l'identité ont souvent des répercussions financières qui vont bien au-delà des mesures correctives initiales. Les organisations sont confrontées à des coûts immédiats tels que... en matière de réponse aux incidents, de reprise après incident et de temps d'arrêt, ainsi que des pertes à long terme telles que la perte de revenus et la baisse de la confiance des clients.

Perturbation opérationnelle

L'identité étant essentielle à l'accès aux systèmes critiques, les attaques peuvent paralyser les activités commerciales à grande échelle. Les employés, les partenaires et les clients perdent l'accès aux applications et aux services, la productivité chute et les efforts de reprise peuvent être entravés.

Atteinte à la réputation

Les atteintes à l'identité peuvent avoir un impact direct sur la confiance des clients et la crédibilité de la marque. La mauvaise publicité et les failles de sécurité perçues peuvent entraîner une perte de clientèle, une baisse de la fidélité et des dommages à long terme difficiles à réparer.

Exposition réglementaire

Lorsqu'un système d'identité est compromis, l'accès non autorisé à des données sensibles peut entraîner de graves conséquences en matière de réglementation et de conformité. Les organisations peuvent se voir infliger des amendes, des poursuites judiciaires et un contrôle accru, notamment dans les secteurs très réglementés comme la finance et la santé.

50%

des organisations ont signalé des failles de sécurité liées à des identités de machines compromises dans l'année dernière.[6]

51%

Ont subi des retards dans le lancement des applications.[6]

44%

ont subi une panne ou une interruption ayant eu un impact négatif sur l’expérience client.[6]

43%

des attaquants ont pu obtenir un accès non autorisé à des données, des réseaux et des systèmes.[6]

6 Rapport sur l'état de la sécurité des identités machine 2025, CyberArk

PERTURBATION RÉELLE LIÉE À L'IDENTITÉ : COMMENT L'INGÉNIERIE SOCIALE A DÉTRUIT LE COMMERCE DE DÉTAIL

En 2025, un groupe de cybercriminels à motivation financière a utilisé des tactiques d'ingénierie sociale coordonnées pour compromettre les systèmes d'identité de plusieurs entreprises de vente au détail au Royaume-Uni, dont la grande chaîne internationale Marks & Spencer.[7]

Plutôt que d'exploiter des failles logicielles, les attaquants ont ciblé les services d'assistance informatique et les processus de support, usurpant l'identité d'employés pour réinitialiser les identifiants, contourner l'authentification multifacteurs et obtenir un accès privilégié. Une fois à l'intérieur, ils ont rapidement étendu leurs privilèges, accédé aux systèmes internes et perturbé les opérations.

Dans certains cas, les attaquants ont exploité cet accès pour déployer des ransomwares, exfiltrer des données et perturber des services critiques pour l'activité démontrant à quel point une compromission d'identité peut rapidement évoluer vers une perturbation opérationnelle à grande échelle.

On estime que ces violations auront un impact financier total de

$592M[7]

Les opérations de vente au détail, les chaînes d'approvisionnement et les systèmes destinés aux clients ont subi des pannes et une dégradation importantes.[7]

46 JOURS:

durée pendant laquelle M&S a suspendu ses ventes en ligne après l'attaque

7 Les actualités des hacker
8 Reuters

COMMENT UN APPEL D'ASSISTANCE TECHNIQUE A CAUSÉ DES MILLIONS DE DÉGÂTS

En 2023, un incident largement médiatisé a paralysé MGM, un important groupe hôtelier et de divertissement, grâce à une ingénierie sociale.

Des attaquants se sont fait passer pour un utilisateur interne et ont contacté le service d'assistance informatique, parvenant à convaincre le personnel de réinitialiser les identifiants et d'accorder l'accès à des comptes privilégiés. Ils ont ensuite étendu leurs privilèges, se sont déplacés latéralement entre les systèmes et ont finalement perturbé les opérations critiques.

Cet exemple renforce un principe clé de la résilience de l'identité : les organisations doivent être prêtes à détecter et à contenir rapidement les attaques basées sur l'identité, à rétablir l'accès de confiance et à reprendre leurs opérations sans interruption prolongée.

L'attaque a coûté plus de ^{100} millions de dollars à l'entreprise.

^{100} millions de dollars de pertes dues à l'indisponibilité du système – ainsi que ^{45} millions de dollars liés à des recours collectifs liés à l'attaque et à une fuite de données survenue en ^{2019}.[9]

Les clients ont exprimé des inquiétudes concernant la sécurité et la fiabilité opérationnelle.[10]

L'incident a déclenché un examen réglementaire et des enquêtes concernant les pratiques de déclaration et de réponse en matière de conformité.[10]

9 Le Record
10 Services d'assurance Inszone

LA SOLUTION : CONSTRUIRE UNE RÉSILIENCE IDENTITAIRE

COMPOSANTES ESSENTIELLES D'UNE STRATÉGIE DE RÉSILIENCE IDENTITAIRE

La résilience de l'identité est la capacité à détecter, contenir et récupérer rapidement des attaques d'identité et autres incidents, tout en maintenant un accès sécurisé et fiable pour les utilisateurs et les applications.

Les éléments clés d'une stratégie globale de résilience identitaire comprennent :

Évaluation proactive pour identifier et hiérarchiser les risques et renforcer la posture de sécurité.

Capacités de surveillance en temps réel et de restauration, permettant une détection et une réponse plus rapides aux attaques basées sur l'identité.

Capacité avérée à restaurer rapidement et de manière fiable l'infrastructure d'identité vers un état sécurisé et fiable.

Visibilité, réponse et récupération à travers les fournisseurs d'identité sur site et dans le cloud.

COMMENT COMMVAULT® OFFRE UNE RÉSILIENCE IDENTITAIRE GLOBALE

Renforcer la résilience des identités exige une approche moderne et unifiée. Commvault Cloud aide les organisations à protéger et à restaurer rapidement leurs systèmes d'identité (notamment Active Directory, Entra ID et Okta) contre les menaces telles que la corruption, la suppression accidentelle et les ransomwares.

Grâce à une approche globale de la résilience des identités, Commvault aide les organisations à évaluer les risques de manière proactive, à détecter et à contenir les menaces en temps réel, et à rétablir rapidement et en toute confiance leurs environnements de fournisseurs d'identité dans un état fiable.

Évaluations de la vulnérabilité

Vous aide à identifier les erreurs de configuration et les vulnérabilités de votre environnement AD – telles que les autorisations excessives et les identifiants sans expiration – et à prioriser les risques grâce à des conseils de correction clairs et exploitables, vous permettant ainsi de renforcer votre sécurité et de réduire les risques.

Récupération granulaire

Permet de restaurer exactement ce qui est nécessaire, jusqu'aux utilisateurs, groupes, unités d'organisation et même attributs individuels spécifiques, sans impact sur l'environnement global.

Protection inviolable

Contribue à protéger les sauvegardes d'identité dans un stockage résistant à toute altération conçu pour empêcher toute modification ou suppression par des identifiants compromis.

Récupération automatisée et orchestrée à grande échelle

Vous aide à récupérer des forêts AD entières, plusieurs domaines et contrôleurs de domaine grâce à des flux de travail coordonnés et automatisés conçus pour des environnements complexes et distribués.

Audit et détection en temps réel

Permet de surveiller en continu les changements d'identité, notamment l'élévation de privilèges, les techniques de persistance et les comportements anormaux, vous permettant d'enquêter et d'annuler instantanément les modifications malveillantes ou non autorisées.

Tests de récupération intégrés

Vous aide à gagner en confiance dans votre préparation aux cyberattaques grâce à des flux de travail de test et de récupération réguliers, qui vous permettent de valider vos plans de récupération et d'améliorer votre résilience.

AU-DELÀ DE L'IDENTITÉ : STRATÉGIE COMPLÈTE DE CYBER RÉCUPÉRATION

Faire face à une cyberattaque ou à une demande de rançon est une expérience traumatisante. La restauration des systèmes d'identité est souvent la première étape, et automatiser ce processus, généralement long et coûteux, peut accélérer la reprise d'activité et permettre une reprise rapide des opérations. L'idéal est que la restauration des identités repose sur la même plateforme que le reste de votre stratégie de reprise après cyberattaques.

La véritable résilience de l'identité va bien au-delà de la simple protection du fournisseur d'identité: il s'intègre facilement à votre stratégie globale de cyber-récupération.

L'unification du processus de récupération et de reconstruction cybernétiques sur une plateforme commune permet une coordination, une automatisation et une orchestration faciles qui vont bien au-delà de la simple récupération d'identité : vous pouvez orchestrer la récupération des applications, des données, des clouds et de l'infrastructure.

Cela aidera vos équipes à travailler ensemble pour reconstruire vos systèmes suite à des cyberattaques et des catastrophes, et développer une résilience qui assure la continuité de vos activités.

Découvrez-en plus sur la résilience d'identité Commvault®

commvault.com | talktous@commvault.com